Headquarters
US Army Armor Center and Fort Knox
Fort Knox, KY 40121
5 February 2002

Security

FORT KNOX INFORMATION SECURITY PROGRAM

Summary. This regulation outlines implementing instructions, responsibilities, and guidance to implement and enhance management of the Fort Knox Information Security Program.

Applicability. This regulation applies to all commanders, directors, supervisors and security managers of commands/organizations supported by Fort Knox, including those organizations with an approved Intra-Service Support Agreement (ISSA) that specifies support will be provided for any facet of Army Regulation 380-5 or 380-10.

Suggested Improvements. The proponent of this regulation is Security Division, G3/Directorate of Plans, Training, and Mobilization, Fort Knox, KY. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to CDR, USAARMC, ATTN: ATZK-PTF, Fort Knox, KY, 40121-5000.

Table of Contents

Page
Chapter 1 - General Provisions and Program Management....4
Section I - Introduction....4
Purpose....4
Definitions....4
Section II - Responsibilities....5
The Commander....5
The Security Manager....6
The Supervisor....7
The Individual....8
Section III - Program Management/Direction....8
Applicability....8
Chief, Security Division, G3/DPTM....8
Section IV - Exceptional Situations....8
Waivers and Exceptions to Policy....8
Section V - Reports and Inspections....9
Reporting Requirements....9
Command Security Inspections....9

Chapter 2 - Local Production of Classified Information and Classification Challenges....11
Section I - USAARMC Originated Classified Information....11
General....11

Producing Classified "USAARMC Owned Information" 11
Section II - Classification Challenges 11
General 11
Receiving or Submitting a Classification Challenge 12

Chapter 3 - Declassification, Regrading, and Destruction 13
Section I - General 13
Section II - Declassification and/or Regrading 13
Section III - Destruction 14
General 14
Destruction Methods 14
Destruction Equipment Available for Command-Wide Use 14

Chapter 4 - Marking 15
General 15
Document Custodians 15
Security Managers 15
Additional Marking Requirements 15
Telephones, Fax Machines, Copiers and Shredders 15

Chapter 5 - Controlled Unclassified Information 17

Chapter 6 - Access, Control, Safeguarding, and Visits 18
Section I - Access 18
Responsibilities 18
Non-Disclosure Agreement (NDA) 18
Section II - Reassignment, Transfer, Retirement, Resignations, Separations, and Termination .. 18
General 18
Reassignments and Transfers 19
Retirement, Resignations, Separations, and Termination 19
Section III - Control Measures 19
Emergency Planning 19
Visitors/Contractors/Consultants 20
Classified Presentations 21
Receipt of Classified Material 22
Section IV - Reproduction of Classified Material 23
General 23
Approval for Reproduction 23
Section V - Additional Inspections 23
Entry Exit Inspection Program (EEIP) 23
M1 Series (Abrams) Tank Security 24

Chapter 7 - Storage and Physical Security Standards 25

Chapter 8 - Transmission and Transportation 26
Section I - Methods of Transmission and Transportation 26
Secret and Confidential Information 26
Section II - Transmission of Classified Material to Foreign Governments 26
Section III - Escort or Handcarrying of Classified Material 26
General 26
Courier Authorization 27

Appendices
A. References 29
B. Example of Exception to Policy/Request for Waiver 31
C. Inspection Checklist 32
D. Entry Exit Inspection Program Procedures 41
E. Example of Courier Duties and Responsibilities Briefing 43
Understanding of Courier Duties and Briefing Verification (DD Form 2501) 46
Understanding of Courier Duties and Briefing Verification (Temporary Written Authorization) 47
Temporary Courier Authorization 48
F. Instructions for Completion of Standard Form 311 49

Chapter 1
General Provisions and Program Management

Section I
Introduction

1-1. Purpose. This regulation establishes internal policy and procedures for inclusion in the local management and execution of the Department of the Army (DA) Information Security Program, prescribed in Army Regulation (AR) 380-5, and is to be used in conjunction with AR 380-5. Additionally, this regulation provides guidance on the duties and responsibilities of local commanders, directors, supervisors and security managers, including those organizations with an approved Intra Service Support Agreement (ISSA) that specifies support will be provided for any facet of Army Regulation 380-5 or Army Regulation 380-10.

1-2. Definitions.

a. Commander: The Commander, Officer in Charge (OIC), Director or head of an agency or activity.

b. Command(s): Commands, directorates, agencies, activities, or areas of responsibility assigned or attached to the US Army Armor Center and Fort Knox, including those organizations with an approved Intra Service Support Agreement (ISSA) that specifies support will be provided for any facet of security governed by Army Regulations 380-5 or 380-10.

c. DOD personnel: Any active, reserve, or National Guard military personnel, or government civilian employee, assigned/attached to a local command, including any person employed by, assigned to, or acting for a local command, including contractors, licensees, certificate holders, and grantees, and persons otherwise acting at the direction of such a command.

d. DA Retention (and destruction) requirements: The disposition instructions applied to a file as directed by AR 25-400-2. AR 25-400-2 implements the provisions of the Federal Records Act (44 USC chapters 21 and 23).

e. Security Manager/(Command)Security Manager (SM): The principal advisor on information security in the command - responsible to the commander for management and administration of the program. The Security Manager is also the key member of the information security program responsible for ensuring the command's security posture is maintained at optimum levels, thus ensuring our national assets are properly protected against subversion, espionage, and pilferage.

f. USAARMC Owned Information: Information, concepts, and requirements, etc that is/are originally developed, visualized, and controlled by USAARMC or a USAARMC Command.

Section II
Responsibilities

1-3. The Commander. Security is a command function. Commanders will effectively manage the information security program within their command. Commanders may delegate the authority to execute the requirements of this regulation, where applicable, but not the responsibility to do so. Security, including the safeguarding of classified and sensitive information and the appropriate classification and declassification of information created by command personnel, is the responsibility of the commander. The commander will:

a. Designate a (Command) Security Manager (SM), primary and alternate, by written appointment. The SM will be of sufficient rank or grade to effectively discharge assigned duties and responsibilities. As a general requirement, the SM will be a commissioned officer, warrant officer, noncommissioned officer (E-7 or above), or government civilian employee (GS-07 or above). In instances where the command is not sufficiently staffed to meet these rank or grade requirements, or a lower rank or grade individual is sufficient to effectively discharge assigned responsibilities, the commander must initiate a request for exception to policy (see paragraph 1-10), in writing, to the Chief, Security Division, G3/DPTM.

b. Establish written local information security policies and procedures and an effective information security education program.

c. Initiate and supervise measures or instructions necessary to ensure continual control of classified and sensitive information and materials.

d. Ensure that persons requiring access to classified information are properly cleared.

e. Continually assess the individual trustworthiness of personnel who possess a security clearance.

f. Ensure the SM has direct access to the appointing commander and the Chief, Security Division, G3/DPTM on matters affecting the information security program.

g. Ensure the SM is afforded security training consistent to the duties assigned.

h. Ensure adequate support and resources are available to allow the SM to manage and administer applicable information security program requirements.

i. Review and inspect the effectiveness of the information security program in subordinate commands.

j. Ensure prompt and appropriate responses are given, or forwarded for higher echelon decisions, any problems, suggestions, requests, appeals, challenges, or complaints arising out of the implementation of this regulation.

k. Ensure the prompt and complete reporting of security incidents, violations, and compromises, related to classified and sensitive information.

l. Ensure prompt reporting of credible derogatory information on assigned/attached personnel, to include recommendations for or against continued access (see USAARMC Pam 380-67).

1-4. The Security Manager (SM). The SM will:

a. Advise and represent the commander on matters related to the classification, downgrading, declassification, and safeguarding of national security information.

b. Establish and implement an effective security awareness and education program that continually encompasses all aspects pertaining to the protection of classified and sensitive information. As a part of this program, ensure each major work and break area has a completed FK Poster 380-5-1 and at least one other security poster visible to all personnel.

c. Establish procedures for ensuring that all persons handling classified material are properly cleared. The clearance status of each individual must be recorded and accessible for verification.

d. Advise and assist officials on classification problems and the development of classification guidance.

e. Ensure that classification guides for classified plans, programs, and projects are properly prepared, distributed, and maintained.

f. Conduct a periodic review of classifications, assigned within the activity, to ensure that classification decisions are proper.

g. Consistent with operational and statutory requirements, review all classified and sensitive documents, in coordination with the Security Division, G3/DPTM and the DOIM, with the goal of continual reduction, by declassification, destruction, or retirement, of unneeded classified and sensitive material.

h. Submit Standard Form (SF) 311 (Agency Information Security Program Data) to Security Division, G3/DPTM per this regulation (see paragraph 1-11).

i. Supervise or conduct security inspections and spot checks and notify the commander regarding the compliance with this regulation, AR 380-5, and other security regulations and directives.

j. Assist and advise the commander in matters pertaining to the enforcement of regulations governing the access, dissemination, reproduction, transmission, transportation, safeguarding, and destruction of classified and sensitive material.

k. Make recommendations, based on applicable regulations and directives, on requests for visits by foreign nationals, and provide security and disclosure guidance if the visit is approved.

l. Ensure the inquiry and reporting of security violations is completed, including compromises or other threats to the safeguarding of classified and sensitive information, per AR 380-5.

m. Ensure proposed public releases on classified and sensitive programs are forwarded to the Chief, Security Division, G3/DPTM per AR 380-5, AR 380-10, and this regulation.

n. Establish and maintain visit control procedures in cases in which visitors are authorized access to classified information.

o. Issue contingency plans for emergency destruction and/or evacuation of classified and sensitive information and material.

p. Be the command's single point of contact to coordinate and resolve classification or declassification problems.

q. Report data as required by this regulation, AR 380-5, and other applicable regulations and directives that apply to information security.

r. Notify the Commander or Security Division, G3/DPTM within 8 hours of any incident discussed in Chapter 10, AR 380-5 and/or thefts involving computer equipment.

1-5. The Supervisor. Supervisory personnel (to include those in command positions) have a key role in the effective implementation of the command's information security program. Supervisors, by example, words, and deeds, set the tone for compliance by subordinate personnel with the requirements to properly safeguard, classify, and declassify, information related to national security. The supervisor will:

a. Ensure subordinate personnel who require access to classified information are properly cleared and are given access only to that information, to include sensitive information, for which they have a need-to-know.

b. Ensure subordinate personnel attend training, understand, and follow, the requirements of this regulation, AR 380-5, as well as, all other local command policies and procedures, concerning the information security program(s).

c. Continually assess the eligibility for access to classified and sensitive information of subordinate personnel and report to the Security Manager any information that may have a bearing on that eligibility.

d. Supervise personnel in the execution of procedures necessary to allow the continuous safeguarding and control of classified and sensitive information consistent with established information security programs.

e. Include the management of classified and sensitive information as a critical element/item/objective in personnel performance evaluations, where deemed appropriate, per Army personnel policy and paragraph 1-5c of AR 380-5. Supervisors should include the protection of classified and sensitive information as a performance evaluation factor or objective for other personnel as the supervisor deems appropriate.

f. Lead by example. Follow command and Army policy and procedures to properly protect classified and sensitive information and to appropriately classify and declassify information as stated in AR 380-5.

1-6. The Individual. All Department of Defense (DOD) personnel, regardless of rank, grade, title, or position, have a personal, individual, and official responsibility to safeguard information related to national security. All DOD personnel will report, to the proper authority, the violations by others that could lead to the unauthorized disclosure of classified and sensitive information. This responsibility cannot be waived, delegated, or in any other respect excused. All DOD personnel will safeguard all information and material, related to national security, especially classified information, which they access, and will follow the requirements of this regulation, AR 380-5, and other applicable regulations.

Section III
Program Management/Direction

1-7. Applicability. This regulation implements local initiatives to enhance the Command's management and execution of the DA information security program and applies to all DOD personnel. This regulation is to be used in conjunction with AR 380-5. Information relating to national security will be protected by DOD personnel and employees against unauthorized disclosure.

1-8. Chief, Security Division, G3/DPTM. As the Command Security Manager for USAARMC and Fort Knox, the Chief, Security Division, G3/DPTM is delegated the responsibility of the implementation and monitoring functions associated with all of the information security programs and requirements.

Section IV
Exceptional Situations

1-9. Waivers and Exceptions to Policy.

a. In the event a command cannot comply with the requirements of this regulation or AR 380-5, a waiver or exception to policy, with full justification, should be requested (example at appendix B).

b. There may be unique situations in which a command may need an exception to the requirements of this publication or AR 380-5; for example, a waiver might be appropriate for a supply or warehouse receiving area that historically receives FEDEX shipments of unclassified materials. A waiver in this instance would eliminate the requirement to use only cleared personnel to screen packages or to store unopened packages in locked containers.

c. All waivers and exceptions to policy will be processed through appropriate command channels to the Chief, Security Division, G3/DPTM for determination on local issues and forwarding to TRADOC for higher-level issues.

Section V
Reports and Inspections

1-10. Reporting Requirements

a. Violations of the provisions contained in AR 380-5 will be promptly reported by Commanders and/or Security Managers to the Chief, Security Division, G3/DPTM, especially those cases involving incidents that can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. See Chapter 10, AR 380-5.

b. Unless otherwise directed, Security Managers will submit, to Security Division, G3/DPTM, a consolidated quarterly report, SF 311, for all elements under their security responsibility. This report should be received no later than the 2d working day of the new quarter. The 4th quarter of each fiscal year the report will be submitted no later than the 1st working day of September, as this will allow a consolidated USAARMC report to be compiled and submitted to TRADOC and ensure the Command's compliance with AR 380-5. (Instructions for SF 311 are at appendix F.)

c. By 4 January each year, Security Managers will report their command's compliance with the annual declassification, regrade, and destruction requirements described in Chapter 3 of this pamphlet.

1-11. Command Security Inspections

a. Each commander will establish and maintain a self-inspection program from their command, and if applicable, a program to inspect their subordinate units.

b. The Security Division, G3/DPTM will conduct mandatory information security program inspections for the Command. (See Appendix C for inspection checklist.) These inspections can be announced or unannounced. A tentative announced inspection schedule will be published at

least 90 days in advance of an inspection. For unannounced inspections, Security Division will notify the commander of the organization to be inspected, a maximum of 48 hours and a minimum of 8 hours, prior to arrival of the inspector(s).

Chapter 2
Local Production of Classified Information and Classification Challenges

Section I
USAARMC Originated Classified Information

2-1. General. As the only authorized Original Classification Authority (OCA) in the Command, the CG, USAARMC is the only person that can apply original classification to "USAARMC owned information."

2-2. Producing Classified "USAARMC Owned Information." When a USAARMC Command generates "USAARMC owned information" that is believed to be classified, the producer of the information must take the following actions:

a. Provide protection to subject information that is equal to, or above, the classification level of the information (i.e., information that is believed to be confidential must be afforded, at a minimum, the same protection as known confidential information, but may be protected at the same level as known secret information).

b. Review Chapter 2 of AR 380-5.

c. Determine if the product must contain classified or potentially classified information.

(1) If it does not, eliminate any such information from the product.

(2) If it does, minimize any such information contained in the product, and be able to fully justify its necessity to the product.

d. Have the information reviewed by your Security Manager, and your immediate supervisor.

e. Forward, through your Security Manager, the product to Chief, Security Division, G3/DPTM for review and coordination.

Section II
Classification Challenges.

2-3. General.

a. One of the information security program's functions is to ensure information is not improperly or unnecessarily classified. AR 380-5 provides guidance for formal challenges to classifications; however, informal questioning is also possible and should be accomplished to resolve any questions prior to submitting a formal challenge.

b. While AR 380-5 provides guidelines for informal and formal challenges of information under a command's OCA, challenges may also be generated to derivative or compiled information. This factor is one of the major reasons to comply with the requirement of making a list of all sources (and if possible, which portion of each source) used to produce these types of information. Additionally, producers of these types of information are encouraged to provide each recipient with a copy of the source list. Providing this will reduce the possibility of a challenge and facilitate easier declassification review.

2-4. Receiving or Submitting a Classification Challenge. Any USAARMC Command, that receives a challenge on information that was locally produced, or wishes to submit a challenge, shall ensure the challenge is properly routed through the Chief, Security Division, G3/DPTM.

Chapter 3
Declassification, Regrading, and Destruction

Section I
General

3-1. The owner (OCA) of any information is the only authority that can decide whether information meets the criteria for continued classification and/or exemption from automatic declassification.

3-2. When a command possesses information that is deemed to no longer be necessary for operational, historical, or reference purposes, and/or has completed it's DA retention requirements (AR 25-400-2), such information shall be destroyed per this publication and AR 380-5.

3-3. To ensure local commands are complying with the provisions of this publication, DA retention and destruction requirements, and AR 380-5, as applied to this chapter, each document, file, etc, containing classified information will be reviewed annually for declassification, regrading, and/or destruction. This annual review will be conducted during the 1st Quarter of each Fiscal Year. Each Security Manager will report compliance with this annual review to the Chief, Security Division, NLT 4 January each year.

Section II
Declassification and/or Regrading

3-4. Upon receipt of instructions/notification of a declassification or regrading action, the Security Manager will ensure the action is completed. If the action affects:

a. An entire document; the markings throughout the document will be changed to reflect the new classification level, the cover page will be annotated to indicate the source of the change, and the instructions/notification will be filed per AR 380-5 and AR 25-400-2.

b. A portion of a document; the affected portions will be remarked to reflect the change, each portion should be annotated to indicate the source of the change, and the instructions/notification will be filed per AR 380-5 and AR 25-400-2.

3-5. If the information is "USAARMC Owned," the Chief, Security Division, G3/DPTM shall be notified, and will guide the producing command through the appropriate, required, procedure.

Section III
Destruction

3-6. General. Classified documents and other material will be retained only if they are required for effective and efficient operation of the command or if their retention is required by law or regulation. Once information has completed it's DA retention requirement or is no longer necessary for operational, historical, or reference purposes, the following actions shall be completed:

a. If the information is "USAARMC Owned" (the CG, USAARMC is the OCA), contact the Chief, Security Division, G3/DPTM for instructions.

b. For US Government information that is not "USAARMC Owned" and non-NATO foreign government information, destroy per AR 25-400-2 and AR 380-5.

c. For NATO information, destroy per AR 380-15.

3-7. Destruction Methods.

a. The equipment or technique used to destroy classified information varies and is dependent on the material make-up of the item containing the classified information. Within this Command, the majority of our classified information is stored or produced on paper, transparencies, CD ROM, or some type of (computer) magnetic media. The approved method of destruction of these, and all, items is described in AR 380-5.

b. Shredding is the most frequently used method of destruction. However, not all shredders meet required specifications. Therefore, the SM will ensure every shredder in their command is clearly marked to indicate the level of information, and type of "media," the shredder is approved to destroy. If the SM is not 100 percent certain of the approved capabilities of a piece of equipment that is going to be used for destruction of classified information, contact the Chief, Security Division, G3/DPTM for assistance.

3-8. Destruction Equipment Available for Command-Wide Use. Security Division, G3/DPTM has authorized equipment available, by appointment, that is capable of destroying paper, CD ROM, non-water soluble (waxed or plastic), computer diskettes, microfilm/microfiches (non-silver based), typewriter ribbons/cassettes, and videotapes.

Chapter 4
Marking

4-1. General. DOD personnel that produce classified or controlled unclassified information are responsible for ensuring the information and the media used to produce, manipulate or store the information is marked per AR 380-5.

4-2. Document Custodians. DOD personnel, particularly classified document custodians, are responsible for reviewing documents in their possession, or they are responsible for storing, to ensure the information was properly marked by the producer.

4-3. Security Managers. Are responsible for:

a. Ensuring all personnel in their command, with a valid clearance, are aware of the marking requirements in AR 380-5.

b. Advising and assisting classified information producers and handlers in complying with the proper marking procedures set forth in AR 380-5.

c. Spot checking information produced, handled, or stored within their command for proper marking procedure application.

d. Reporting to the Commander and/or the Chief, Security Division, G3/DPTM the following:

(1) DOD personnel, within their command, who refuse to adhere to the marking requirements of AR 380-5.

(2) Any incident that resulted or may have resulted in the disclosure of improperly marked information to an unauthorized individual or organization. (See Chapter 10, AR 380-5)

4-4. Additional Marking Requirements. The following marking requirements shall be observed in this command:

a. Page marking: Mark or stamp the top and bottom of the back of the last page of a classified document with the same markings as the first page.

b. File folders: Conspicuously mark or stamp the front and back of file folders containing classified material. These markings shall be placed so that the classification of the contents is readily visible when the folder is placed in the security container drawer.

4-5. Telephones, Fax Machines, Copiers and Shredders.

a. All telephones and Fax machines will have a DD Form 2056 affixed to them. Secure telephones and secure Fax machines will have a modified version, reminding the user to always ensure the sending and receiving systems are in the secure mode prior to transmitting.

b. All copiers will be clearly marked to indicate the level of information authorized to be reproduced on the equipment. If the equipment is authorized to reproduce classified material, see Chapter 6, Section III for additional markings.

c. All shredders will be clearly marked to indicate the level of information authorized for destruction.

Chapter 5
Controlled Unclassified Information

5-1. While not classified, CUI protection is a must. Of all the different types of information that require protection, controlled unclassified information (CUI) is the least recognizable and is also a high payoff target for individuals/organizations to gain unauthorized disclosure.

5-2. On a daily basis, we handle a tremendous amount of CUI, particularly FOUO, sensitive information (Computer Security Act of 1987), and technical documents. A great percentage of CUI handlers are not aware of proper handling and protection requirements.

5-3. Producers of compiled information must maintain a list of all sources, and provide this list, on demand to the Disclosure Officer or the Freedom of Information Act Office.

5-4. In this command, there are only two offices authorized to release CUI to non-DOD entities:

a. The Freedom of Information Act Office (DOIM).

b. The Disclosure Officer (G3/DPTM, Security Division).

5-5. Commanders and security managers must aggressively educate all members of their command on:

a. What is CUI?

b. Where it exists in their command.

c. Proper handling procedures. (AR 25-55, AR 70-11, AR 380-5, AR 380-10, AR 380-19, and local regulations/procedures.)

Chapter 6
Access, Control, Safeguarding, and Visits

Section I
Access

6-1. Responsibilities.

a. As a condition to providing access to anyone, the holder of classified information must ensure the recipient:

(1) Has need-to-know.

(2) Has clearance authorization (see para 6-7 for contractors, consultants, and visitors).

(3) Understands the information is classified.

(4) Knows how to protect the information.

(5) Has the ability to protect the information.

(6) If transporting the information to another location, has the proper credentials.

b. If any one of these does not exist, access to the information should be delayed, and the holder's security manager is notified for guidance.

6-2. Non-Disclosure Agreement (NDA). Security managers will maintain documentary proof that DOD Civilians and locally hired DOD consultants have executed an NDA. The preferred proof is a photocopy of the signed NDA; however, a Standard Form 75 or a DA Form 200, confirming receipt, indicating that an NDA is present or has been received for inclusion, in the employee's official personnel file, is acceptable.

Section II
Reassignment, Transfer, Retirement, Resignations, Separations, and Termination.

6-3. General.

a. All DOD personnel and local hire consultants will outprocess through the security manager.

b. All personnel that have been designated on orders as a courier will have their orders revoked immediately.

c. All personnel that have been issued a DD Form 2501 (Courier Authorization Card) must turn it in to their security manager.

6-4. Reassignments and Transfers.

a. Military Personnel. The security manager will forward the "local" file copy of the individual's NDA to the gaining security manager. This action can be accomplished either by providing the copy to the soldier for handcarrying or by official mail. If the soldier is handcarrying, the copy should be placed in an envelope and addressed to: S2/Security Manager.

b. Civilian Personnel. If the security manager is maintaining a copy of the NDA, the same procedures described in 6-4a apply.

6-5. Retirement, Resignations, Separations, and Termination. All DOD personnel and local hire consultants will be debriefed by the security manager. The debriefing will be conducted, documented, and filed per AR 25-400-2, AR 380-5, and AR 380-67.

Section III
Control Measures

6-6. Emergency Planning.

a. All commands with classified material shall establish emergency plans that provide for the protection of classified material in a manner that will minimize the risk of personal injury or loss of life to personnel. In the case of fire, or natural disaster, this requires the immediate placement of authorized personnel around the affected area, pre-instructed and trained to prevent removal of classified material and reducing casualty risk.

b. Post emergency plans in a conspicuous place, such as on the wall near the storage container(s) or on the container itself. Such plans shall provide for emergency destruction or evacuation to preclude capture, compromise, or loss of classified material when determined to be required. This determination shall be based on an overall common sense evaluation of the following factors:

(1) Level and sensitivity of classified material held by the activity.

(2) Sensitivity of operational assignment.

(3) Potential for aggressive action of a hostile entity.

c. When preparing emergency plans, consideration shall be given to the following:

(1) Reduction of the amount of classified material held by your command.

(2) Transfer of as much retained classified material to an "other than paper" type of media.

(3) Emphasis on the priorities for destruction/evacuation, designation of personnel responsible for destruction/evacuation, and the designation of places and methods of destruction/ evacuation. Additionally, if any destruction site or any particular piece of destruction/evacuation equipment is to be used by more than one activity or entity, the order or priority of use of the site or equipment must be clearly delineated.

(4) Identify the individual(s) authorized to receive/disseminate the execution order, once the G3/DPTM, Security Division has determined an emergency destruction/evacuation is to begin. Additionally, how the order will be disseminated to all subordinate elements (emergency plans will clearly identify the position titles of these individuals).

(5) Authorization for the senior person present to deviate from established plans when circumstances warrant.

(6) Emphasis on the importance of implementing the plan early to preclude loss/ compromise of material. The effect of premature destruction is considered inconsequential when measured against the possibility of compromise.

d. Classified material holdings shall be prioritized for emergency planning. Priorities should be based upon the potential effect on national security, should such holdings fall into unauthorized hands. The following guidelines are provided:

(1) Priority One. (Top Secret) Exceptionally grave damage. (Secret SAPs should also be labeled as a priority one.)

(2) Priority Two. (Secret) Serious damage.

(3) Priority Three. (Confidential) Damage.

e. In determining the method of destruction of other that Priority One (Top Secret) material, any method specified for routine destruction of any other means that will ensure positive destruction of the material may be used. Ideally, any destruction method should provide for early attainment of a point at which the destruction process is irreversible.

6-7. Visitors/Contractors/Consultants

a. On occasion, personnel from this command visit activities and organizations off of the installation. Many times these visits involve classified information/material, creating a need to certify individual security clearance information. To facilitate the certification of security clearances, security managers will prepare and authenticate FK Form 5060-E, May 2001.

b. When a command is contacted by, is inviting, hosting, or sponsoring, a visit of any person or organization, the security manager shall be notified. The Security Manager will:

c. Notify Security Division, G3/DPTM when the visit involves foreign personnel. Information on visits by foreign persons/organizations will be handled per AR 380-10.

d. Ensure the procedures of Chapter 6, AR 380-5 are adhered to, if the pending or proposed visit is anticipated to involve access to classified material/information. (FK Form 5060-E, May 2001, may be used to verify clearance/access information.)

e. Maintain information on all visits to their organization, this information will be retained and filed per AR 25-400-2 (Foreign Visitors - 380-10d and US Visitors - 600-25b).

f. Maintain the following for contractors/consultants working in your command and requiring access to classified material:

(1) Confirmation of security clearance and level of clearance.

(2) Confirmation of execution of nondisclosure agreement.

(3) Copy of the contracts "statement of work" (to assist in establishing need-to-know).

(4) Contact information for the Contracting Officer Representative, the Security Manager of the US Government Sponsoring Agency, and the Security Manager for the contracted organization.

6-8. Classified Presentations (meetings, conferences, classes, lectures, and other presentations). Command activities that hold or sponsor any type of classified presentation will appoint a security representative to be responsible for the overall security at the site of the presentation. The security representative will ensure:

a. The date, location and subject of the presentation are furnished to Security Division, G3/DPTM at least 3 working days prior to commencement.

b. Conversations or discussions involving classified material are not held in areas where they can be overheard by unauthorized personnel. This includes ensuring that public address systems are set at a level which precludes classified discussions/presentations from being overheard outside of the presentation area.

c. Individual speakers/presenters will announce the security classification of the subject matter at the beginning and end of their presentation.

d. All personnel are evacuated from the presentation room, prior to initiating an access roster check.

e. Access rosters (name, rank, SSN, clearance, and organization) to verify authorized attendees are compiled and used at a controlled entrance point.

f. Attendees must be identified by presenting a picture ID (military/civilian employee ID card, passport, drivers license, etc.) before admittance into the presentation area. Support personnel (i.e., guards, monitors, etc.) will verify personal information by comparing the access roster and the presented ID. If there are discrepancies, the attendee must be referred to the security representative. Under no circumstances will the attendee be allowed to enter that presentation area until the security representative verifies their authorization to attend.

g. Doors and windows are closed and covered during the presentation.

h. Briefcases, cameras, video recorders, computers, cell phones, beepers, electronic recording devices, or any other similar electronic device(s) will not be allowed to enter the presentation area.

i. Care is exercised to reduce the possibility of clandestine surveillance listening devices being installed in areas where classified information is discussed/presented. A physical check will be made of the area to detect any obvious device that could be used to transmit or record the presentation (i.e., adjacent rooms, hallways, heating/AC vents or ducts, inside/outside of perimeter walls, window ledges, dropped/false ceilings, etc.).

j. Note taking, unless strictly controlled, is prohibited.

k. Sufficient, appropriately cleared guard/monitor personnel are pre-positioned at all entrances, exits, and adjacent areas to prevent unauthorized access or loitering.

l. The presentation site is checked immediately following the departure of all attendees to ensure no classified material has been inadvertently left in the area.

6-9. Receipt of Classified Material. All commands will establish procedures for protecting incoming official first class, registered mail, and express mail/packages until a determination is made on whether classified information is contained therein. As part of these procedures, official first class mail recipients/openers and registered/express mail/package recipients/openers will be appointed on orders.

a. Individuals appointed as recipients/openers of official first class mail must possess, at a minimum, a Confidential clearance.

b. Individuals appointed as recipients/openers of registered/express mail/packages must possess, at a minimum, a Secret clearance.

Section IV
Reproduction of Classified Material

6-10. General. Unnecessary, non-mission essential, reproduction of classified material increases the possibility for security violations and compromise.

6-11. Approval for Reproduction.

a. Commanders that feel their commands have a requirement to make mission essential reproductions of classified material will submit a written request, to Security Division, G3/DPTM, ATTN: ATZK-PTF-D, for authorization to reproduce classified material. This request shall:

(1) Include a justification for reproduction authority.

(2) List the equipment to be used. (Make, model, serial number, etc.)

(3) Denote the equipment's location.

(4) Provide the name or position of the individual to be designated as the Classified Material Reproduction Control Officer.

(5) Include a copy for the internal control procedures to be used.

(6) Provide a time period the request is to cover. (May not be more than 12 months.)

b. Approval for the reproduction of Top Secret, SAPs, NATO, and other categorized material may only be granted by the appropriate, installation, control officer. However, such requests shall be submitted through Security Division, G3/DPTM, to the proper control officer.

c. All reproduction equipment will be clearly marked, with the appropriate notice, reflecting the highest level of information that may be duplicated on it. The following are stocked at the DOIM Forms Warehouse or may be available at Security Division, G3/DPTM:

(1) TRADOC Label 1016R (Classified Reproduction Notice) for equipment authorized to reproduce classified material.

(2) TRADOC Form 1017R (Unclassified Reproduction Control Notice) for equipment not authorized to reproduce classified material.

Section V
Additional Inspections.

6-12. Entry Exit Inspection Program (EEIP).

a. The EEIP will be managed and executed at the installation level. The Security Division, G3/DPTM will randomly conduct EEIP inspections. Prior to conducting an EEIP inspection, the security manager will be given a minimum of 4 working hours notice. This does not prevent commands from conducting EEIP inspections on their own. Instructions and procedures for conducting these inspections are at Appendix D.

b. Security managers are responsible for EEIP awareness and education. This should be accomplished by inclusion in the command's SOP and annual security training.

c. Security managers are responsible for ensuring FK Poster 380-5-8 is clearly, and continually, posted at the entrance(s) of their building(s) that house classified material.

6-13. M1 Series (Abrams) Tank Security. Although this is a physical security requirement, breeches of the external armor are reportable as a potential compromise under AR 380-5. Further information is contained in the installation Force Protection and/or Physical Security Plans.

6-14. Requirements and procedures for additional inspections relating to the DA Information Security Program will be coordinated, under separate cover, with the affected command(s).

Chapter 7
Storage and Physical Security Standards.

7-1. All elements in this command will contact Security Division, G3/DPTM (ATZK-PTF-D), prior to purchasing or turning in any equipment discussed in Chapter 7, AR 380-5. This is strictly a cost savings measure as this office may have information on a requirement change, or the location of a command that has or desires transferable equipment.

7-2. Security Managers are responsible for changing combinations on security containers storing classified material. Assistance or training for changing combinations may be obtained by contacting Security Division, G3/DPTM.

7-3. Locksmiths will not be utilized to assist in routine combination changes. In cases where locksmith services are required, security managers must coordinate with Security Division, G3/DPTM prior to initiating the request.

7-4. Commands having more than one security container will designate one container as the master container. The master container will contain Part 2 and 2a of SF 700 for all other security containers. The Part 2 and 2a of the master containers SF 700 will be maintained in the master container of the next higher command, if the command is located on this installation, otherwise they will be maintained in the DOIM Classified Control Office, Building 1227. The only authorized exception is for containers storing 2-person control material; for these containers complete only Part 1, SF 700.

Chapter 8
Transmission and Transportation

Section I
Methods of Transmission and Transportation

8-1. Secret and Confidential Information:

a. If US Postal Service services cannot meet an urgent requirement, DOD policy authorizes the use Federal Express (FEDEX). This service is only authorized for use within CONUS and only between DOD commands. FEDEX is not authorized to transmit material to contractors or non-DOD agencies. Additionally, classified COMSEC material, Sensitive Compartmented Information (SCI), or classified SAP material will not be transmitted using FEDEX.

b. Material to be shipped will be prepared per Chapter 8, AR 380-5. The sender must ensure that a proper address is used to ensure the package goes to a cleared person, with appropriate need-to-know, or who will ensure delivery of the package to the person or office with the need-to-know. After packaging, classified material must be taken to the Fort Knox Post Office (Bldg. No. 1359, Post Locator side) for processing by postal officials. Under no circumstances will classified FEDEX packages be dropped off in a FEDEX drop box.

c. Packages being shipped via FEDEX will be shipped Monday through Thursday only.

d. Customers will retain the receipt given them by postal officials until notification is received that the material has arrived at its final destination. Classified Document Accountability Record, DA Form 3964 will be utilized and retained per AR 380-5.

Section II
Transmission of Classified Material to Foreign Governments

8-2. Prior to release or transmission of classified information or material, approval must be obtained from the installation Foreign Disclosure Officer. For further information/assistance contact Security Division (ATZK-PTF-D), G3/DPTM.

Section III
Escort or Handcarrying of Classified Material

8-3. General.

a. Within the confines of Fort Knox, personnel that hand carry/transport classified material, outside of their immediate work area (to another building) must have in their possession either a DD Form 2501 (Courier Authorization Card) or an original copy of a courier authorization letter or memorandum. The individual command's Security Manager is the only issuing authority for

either of these documents. The following requirements pertain only to classified material being transported within the confines of Fort Knox:

(1) Classified material shall only be transported from one working area or building, directly to another working area or building. And only when absolutely necessary.

(2) When transporting classified material between working areas or buildings, the material must at a minimum have the appropriate cover sheet attached (inner wrapping) and be enclosed in a sealed opaque envelope or container (outer wrapping). A locked briefcase qualifies as an outer wrapping.

b. Authorization to hand carry classified material off the installation using commercial conveyance or outside the continental US is reserved for the Chief, Security Division, G3/DPTM. These authorizations will only be granted when all other authorized means of transmission have been evaluated and cannot be utilized to complete a critical mission requirement. For further information and procedural guidance, contact Security Division, G3/DPTM.

8-4. Courier Authorization.

a. Security Managers:

(1) Must, prior to issuance of any courier authorization, verbally brief the individual on the duties, responsibilities, and limitations of authorization, pertaining to their specific courier authorization. An example of what this briefing might contain is located in appendix E.

(2) Upon completion of the verbal briefing, the designated courier must sign the appropriate statement (appendix E), to verify they have been briefed and understand their responsibilities. Security Managers retain the statement with the individual's DA Form 1378.

(3) Are authorized to sign DD Forms 2501 and courier authorization letters/ memorandums for their command members determined to have a need to handcarry classified material within the continental US and are traveling only by government conveyance. All other authorizations must be granted by Security Division, G3/DPTM.

b. DD Form 2501 is an accountable form and is only available from Security Division, G3/DPTM. DD Form 2501 will:

(1) Be used when ground transportation or military air is the mode of travel.

(2) Not be used when handcarrying classified material aboard commercial aircraft.

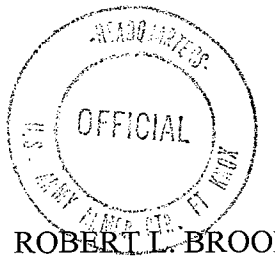
(3) Be issued for a period not to exceed 2 years. Upon expiration of the form or reassignment, transfer, retirement, resignation, separation, or termination of an individual issued a DD Form 2501, the card will be returned to the security manager for destruction.

(4) Semi-annually, be inventoried on a "show" basis.

(5) Be limited to personnel that frequently handcarry classified information or material.

c. Written authorization from the security manager, is an acceptable means of courier identification on the installation. An example of written authorization is at appendix E.

FOR THE COMMANDER:



ROBERT L. BROOKS
Director, Information Management

OFFICIAL:
ROBERT T. GAHAGAN
Colonel, GS
Chief of Staff

DISTRIBUTION:
A

CF:
DCG, USAARMC

Appendix A
References

DOD Publications

DOD 4525.6-M, DOD Postal Manual (Vol II), February 1987

DOD 5200.1-R, DOD Information Security Program Regulation, 1 January 1997

Army Regulations

AR 25-55, The Department of the Army Freedom of Information Act Program, 14 November 1997

AR 25-400-2, The Modern Army Record Keeping System (MARKS), 1 October 2001

AR 380-5, Department of the Army Information Security Program, 29 September 2000

AR 380-10, Foreign Disclosure, Technology, Transfer, and Contacts with Foreign Representatives, 15 February 2001

AR 380-19, Information Systems Security, 27 February 1998

AR 380-49, Industrial Security Program, 15 April 1982

AR 380-67, The Department of the Army Personnel Security Program, 9 September 1988

AR 380-381, Special Access Programs (SAPs), 12 October 1998

AR 381-12, Subversion and Espionage Directed Against the US Army (SAEDA), 15 January 1993

AR 525-13, Antiterrorism/Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources, 10 September 1998

AR 530-1, Operations Security (OPSEC), 3 March 1995

TRADOC

Reg 525-13, TRADOC Force Protection Program (FPP), December 1997

Memo, ATBO-JC, subject: Transmission of DOD Classified Material via Federal Express (FEDEX), 20 December 1994

Fort Knox Reg 380-5 (5 Feb 02)

Local Regulations/Policies

Fort Knox Reg 25-70, Procedures for the Entry of Information into the Fort Knox World Wide Web (WWW) Site/Internet and Use of Fort Knox Communications Resources, 12 April 2000

USAARMC Pam 380-67, Personnel Security Program, 21 October 1994

Forms/Labels/Posters

Standard Form 75, Request for Preliminary Employment Data

Standard Form 311, Agency Security Classification Management Program Data

Standard Form 312, Classified Information Nondisclosure Agreement (NDA)

Standard Form 700, Security Container Information

DD Form 2056, Telephone Monitoring Notification Decal

DD Form 2501, Courier Authorization Card

DA Form 200, Transmittal Record

DA Form 3964, Classified Document Accountability Record

TRADOC Form 1016-R, Reproduction Control Notice (Classified)

TRADOC Label 1017-R, Reproduction Control Notice (Unclassified)

FK Poster 380-5-1-E, Your Security Team

FK Poster 390, Reproduction of Classified Material Prohibited

FK Poster 380-5-8, Entry/Exit Inspection

Appendix B
Example of Exception to Policy/Request for Requirement Waiver

ATZK-XXX (380)

MEMORANDUM FOR Security Division, G3/DPTM (ATZK-PTF)

SUBJECT: Request for Requirement Waiver

1. Request you grant a waiver for the "security manager grade" requirement listed in paragraph 1-4a of Fort Knox Reg 380-5.

2. After reviewing our current staffing level, I have determined that I do not have any military or civilian personnel assigned that have either a reasonable amount of retainability or the ability to effectively discharge the duties of a security manager and/or that meet said grade requirement.

3. I am aware that the Information Security Program is my responsibility, and if granted this waiver, I will ensure the appointed security manager receives the full cooperation of my organization.

I. M. AWARE
DAC
Director, Mastermind Development

Appendix C
Inspection Checklist to Fort Knox Reg 380-5

1. REFERENCES

AR 25-400-2, The Modern Army Records Keeping System, October 2000.

AR 380-5, DA Information Security Program, September 2000.

AR 380-10, Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives, February 2001.

AR 380-67, Personnel Security Program, September 1988.

AR 381-12, Subversion and Espionage Directed Against the US Army, January 1993.

AR 525-13, Antiterrorism Force Protection AT/FP, September 1998.

AR 530-1, Operation Security, March 1995.

DA Pam 25-16, Security Procedures for Secure Telephone Unit, Third Generation (STU-III), April 1993.

Fort Knox Reg 380-5,

USAARMC Pam 380-67, October 1994.

Are the listed references readily available to the Primary and Alternate Security Managers?

REMARKS:_____

_____

2. APPOINTMENTS AND AUTHORIZATIONS

a. Has a Primary and Alternate Security Manager been appointed in writing? And do those appointed meet the grade/rank requirement? If not, has an exception to policy been granted? (AR 380-5, para 1-6/Fort Knox Reg 380-5, para 1-4)

b. Have individuals with appropriate clearances been appointed as official first class (confidential) and registered/express mail (secret) openers? (AR 380-5, CH 6 and Fort Knox Reg 380-5, para 6-9.)

c. Has an official been designated to authorize reproduction of classified material? (Fort Knox Reg 380-5, para 3-11)

REMARKS:_____

_____

3. ACCESS

a. Have Classified Information Nondisclosure Agreements (SF 312) been executed on all government personnel with access to classified information? (AR 25-400-2, AR 380-5 CH 6, and Fort Knox Reg 380-5 CH6 Section I)

(1) Are SFs 312 completed as a condition of access?

(2) Are SFs 312 properly prepared and maintained?

(3) Are SFs 312 for civilian personnel placed in their OPF?

(4) Are SFs 312 for military personnel forwarded to: PERSCOM or EREC?

(5) Are records of debriefings properly maintained?

b. Does the security manager have the following for all contract/consulting personnel working in their command: (Fort Knox Reg 380-5 CH6 Section II)

(1) Confirmation of security clearance and level of clearance.

(2) Confirmation of execution of nondisclosure agreement.

(3) Copy of the contracts "statement of work" (to assist in establishing need-to-know).

(4) Contact information for the Contracting Officer Representative _____, the Security Manager of the US Government Sponsoring Agency _____, and the Security Manager for the contracted organization _____.

c. If the command has visitors, are the procedures of Chapter 6, AR 380-5 adhered to, if the visit involves access to classified material/information? (Fort Knox Reg 380-5 CH6 Section II)

d. Is visitor information: (FORT KNOX Reg 380-5 para 6-7)

(1) Retained on all visits to the command?

(2) Filed per AR 25-400-2 (Foreign Visitors - 380-10d and US Visitors - 600-25b).

e. Is there a current list of all personnel authorized access to Top Secret Info?
- Are these individuals read-on to SCI?
- Have they attended the required annual SCI update brief?

REMARKS:_____

_____

4. SECURITY POLICIES AND PROCEDURES

a. Have supplemental security policies and procedures been developed for this activity? (AR 380-5 and Fort Knox Reg 380-5 para 1-4)

b. Do the policies and procedures include:

(1) Guidance on access?

(2) A security education program?

(3) Information on duplication/copying classified info?

(4) Guidance on violations/compromises/infractions?

(5) Information on destruction of classified/controlled unclassified info?

(6) Guidance on hand carrying classified?

(7) Guidance on sending classified mail/packages?

(8) Guidance on receipt of mail/packages?

(9) STU III/STE telephone use?

(10) Conducting classified meetings, conferences, etc?

(11) Required travel briefings?

(12) Guidance about visitors/contractors/consultants?

(13) Emergency Action Plans for evacuation and destruction?

REMARKS:_____

_____

5. SAFEGUARDING

a. Has the activity conducted self-inspections/spot checks to determine the effectiveness of their security programs? (AR 25-400-2, AR 380-5, Fort Knox Reg 380-5 para 1-12)

(1) Are these self-inspections/spot checks recorded?

(2) Are these records properly maintained?

b. Does the command have a website/webpage/homepage? (AR 380-5, App E/FK Reg 25-70)

(1) Is it accessible independent of the Fort Knox Homepage? If so, is there a banner that complies with AR 380-5, Appendix E?

(2) Has the information been appropriately staffed for release?

c. Are procedures in place to ensure the requirements for conducting classified meetings/conferences accomplished properly? (Fort Knox Reg 380-5 CH6 Section II)

d. Do all telephones (and FAX machines) have a DD Form 2056 affixed to them? (Fort Knox Reg 380-5 para 4-5)

e. Does the command have a STU III/STE telephone or classified FAX? (Fort Knox Reg 380-5 para 4-5)

(1) Do they have a modified version of DD Form 2056 affixed to them? Additionally, FAX machines should also be labeled indicating the level of information authorized to receive. (Fort Knox Reg 380-5 para 4-5)

(2) Is the access and storage for each crypto ignition key properly employed? (DA Pam 25-16)

(3) Are proper security procedures employed when using this equipment? (AR 380-5 CH6)

REMARKS:_____

_____

6. DOCUMENT MARKINGS
(AR 25-400-2, AR 380-5 CH4, Fort Knox Reg 380-5 CH2 and 3)

a. Are classified documents properly marked with the overall classification level?

b. Are interior pages of classified documents properly marked?

c. Is the classification authority properly identified on the classified by/derived from line?

d. Are downgrading or declassification instructions properly displayed on the document?

e. If the command created the document:

(1) Under the CG's OCA authority, does the document reflect the creating organizations name, justification for classification and date of classification decision.

(2) From derivative sources, does the record copy have a list of all sources?

f. Are working papers dated when created, safeguarded and either destroyed or finalized after 180 days?

g. Are file folders and binders containing classified material marked with the overall classification level of the information contained inside?

h. Are classification challenges made to the proponent when an incorrectly marked document is received?

REMARKS:_____

_____

8. DESTRUCTION.
(AR 25-400-2, AR 380-5 CH3 and 6, Fort Knox Reg 380-5 CH3 and 4)

a. Are approved methods being utilized for the destruction of classified material?

b. Are all shredders clearly labeled to reflect the level of information authorized for destruction in the equipment?

c. Is the activity destroying documents that are 5 years old, or older, that are not permanently valuable records of the government?

d. Has the annual classified document clean-out day been accomplished?

e. Are destruction certificates and witnesses used and maintained as required?

REMARKS:_____

_____

9. REPRODUCTION. (Fort Knox Reg 380-5 CH4 and 6)

a. Has equipment been approved to reproduce classified information?

b. Are appropriate notices and procedures posted on or near equipment used to reproduce classified information?

c. Is a reproduction control sheet used to log the amount of classified material reproduced?

d. Is reproduction of classified material limited held to an only mission essential standard?

REMARKS:_____

_____

10. SECURITY CONTAINER MANAGEMENT
(AR 380-5 CH 6 and 7, Fort Knox Reg 380-5 CH6 and 7)

a. Is classified information properly stored in GSA approved security containers?

b. Are SFs 700 posted in the mechanical drawer of each security container indicating individuals with knowledge of the combination and the contents?

c. Have containers used for storage of classified information or material been designated and a number or symbol annotated on the SF 700 affixed to the inside of each container?

d. Are safe combinations changed at least annually and as otherwise required?

e. Was the combination changed by the security manager?

f. Are safe combinations maintained in a master safe?

g. Are records of combinations assigned a security classification equal to the highest category of classified material authorized to be stored in the container?

h. Is the master safe combination maintained at DOIM?

i. Is the SF 702 being filled out properly, indicating each time the security container is opened, closed, and checked?

j. Are end of the day security checks conducted and recorded on SF 701?

k. Is there an Emergency Action Plan (EAP) posted on each container?

l. Are priority stickers placed inside each drawer?

m. Are magnetic signs indicating when the container is opened or closed located on the front of each container?

n. Are security containers, ready for turn-in, inspected for any left over classified and are the combinations reset to the factory set combination (50-25-50)? Are signed statements affixed to these containers attesting to the combination settings and inspection for classified material for the Property Book Officer?

REMARKS:_____

_____

11. TRANSMISSION (AR 380-5 CH 7 and 8, Fort Knox Reg 380-5 CH8)

a. Are Courier Authorization Cards (DD Form 2501) issued only to those individuals who carry classified information on a frequent basis?

b. Are Courier Authorization Cards properly controlled and inventoried? Control Log, current inventory, destruction and outprocessing?

c. Are classified couriers briefed and given a statement on their responsibilities before being assigned a courier card (DD Form 2501) or courier orders? Are their signed statements being maintained in their security personnel file?

d. Are issued courier cards only valid for 2 years or less, and are individual needs to carry classified being reevaluated annually?

e. Are all assigned personnel aware of proper methods of transportation of classified information/material? Are proper controls such as double wrapping, registered mail, locking brief cases being enforced?

f. Is a travel security and espionage briefing given to couriers traveling off the installation.?

g. Are couriers traveling OCONUS given a courier authorization letter to travel abroad with classified aboard a commercial aircraft?

REMARKS:_____

_____

12. SECURITY EDUCATION AND AWARENESS
(AR 25-400-2, AR 525-13, AR 530-1, AR 380-5 CH9, Fort Knox Reg 380-5 CH6)

a. Does the command have a security education program that meets the criteria/objectives of AR 380-5, Chapter 9? (Inspector has the option of asking "check on learning" security related questions to members of the command.)

b. Does the program provide for continual re-enforcement of security?

c. Are there records, reflecting date, subject, and attendees, for all education program sessions?

d. Does each attendee's security file reflect education and awareness sessions attended?

e. Are the sessions tailored to meet the education/awareness needs of the individual as well as the activities mission?

(1) Are initial briefings being conducted before access is granted?

(2) Are debriefings being conducted?

(3) To ensure all personnel are aware of security procedures and individual responsibilities regarding basic security disciplines?

(4) Are all personnel receiving a biennial SAEDA briefing?

(5) Are all personnel receiving an annual OPSEC briefing?

(6) Are all personnel receiving an annual Information Security Briefing?

(7) Are individuals traveling abroad or PCS'ing abroad receiving a foreign travel and force protection briefing? For those with access to SCI, have they received an SCI foreign travel briefing?

(8) When an individual is authorized to handcarry or escort classified material, locally, inside CONUS and OCONUS?

(9) When an individual is granted access to SCI, SAP, NATO, CNWDI, etc?

(10) Are supervisors informed of their responsibilities?

(11) Are employees made aware of individual/co-worker responsibilities?

f. Are security awareness posters sufficiently displayed throughout the activity to remind personnel of their responsibility to safeguard classified material?

g. Is FK Poster 380-5-1 posted on the command's bulletin boards to identify the command's Security Manager?

h. Is FK Poster 380-5-8 posted in clear view at all entrances/exits of the building to continually remind individuals of the possibility of an Entry/Exit Inspection?

REMARKS:_____

_____

13. VIOLATIONS AND INFRACTIONS
(AR 25-400-2, AR 380-5 CH10 and Fort Knox Reg 380-5 CH1)

a. Are possible and actual security violations being reported immediately to the Security Manager/Commander and Security Division, G3/DPTM?

b. Are preliminary inquiries conducted per policy and regulation? Is a system in place to conduct preliminary inquiries?

c. Are completed preliminary inquiries maintained on file for 2 years?

REMARKS:_____

_____

Appendix D
Entry Exit Inspection Program Procedures

1. WHO IS TO BE INSPECTED. All individuals entering or exiting the building during the inspection period, regardless of rank or grade are subject to inspection by designated personnel.

2. THE PURPOSE OF THE INSPECTION. Inspections will be conducted for the sole purpose of detecting and deterring the unauthorized introduction or removal of classified information. Inspections will not be used to target, single out, harass, or otherwise treat any individual differently than other persons entering and exiting the activity.

3. WHAT TO LOOK FOR. Inspector personnel will examine envelopes, packages, diskettes, diskette containers, and other ADP media, tapes, films, microfiche, etc., likely to contain classified material. Sealed envelopes and packages are also subject to inspection. If an individual refuses to open a sealed envelope, or will not allow the inspector to do so, he or she will be asked for written courier orders (or DD Form 2501) or other proof of authorization to hand carry classified material. If the person does not have such authorization, the incident will be recorded, and they will be referred to the Security Division, G3/DPTM for further action.

4. WHAT IS TO BE INSPECTED. While inspections are being conducted, authorized personnel will inspect all briefcases, luggage, athletic bags, packages, shoulder or handbags and other similar containers carried into and out of the activity by visitors and employees. Inspectors will not open or handle a woman's shoulder/hand bag. The woman will be asked to open her bag and rearrange or remove all items necessary to allow the inspector to view the contents. Personnel conducting the inspections are expected to use discretion in inspecting any item that could reasonably be expected to contain classified information.

5. WHAT WILL NOT BE INSPECTED. Inspectors will not search items that are obviously personal, such as wallets, change purses, clothing or cosmetic cases. Inspector personnel will not inspect the individual's person.

6. HOW TO INSPECT. Personnel designated to conduct inspections will be polite, professional and courteous at all times. During the designated period, inspectors will inform each person to be inspected of the requirement to inspect items brought into and out of the facility.

7. METHOD OF INSPECTION. Either of two methods will be used: random or continuous. One the method is determined by the security official, inspectors will consistently follow that method during that particular inspection period. (i.e. if a random inspection of every third person is selected, then every third person will be inspected). An inspection log will be maintained by the inspectors and turned into the inspection supervisor at the end of the inspection period. This log will consist of:

a. Name of inspector.

b. Date, time, and location of inspection.

c. Method of inspection (random or continuous).

d. Sign in and out sheet for all personnel entering or exiting the activity during the inspection period. If random method is the type of inspection chosen, inspector will place and asterisk beside the name of persons inspected.

e. Comments/problems.

8. PROCEDURES IN THE EVENT CLASSIFIED MATERIAL IS DISCOVERED. If classified information is discovered, the individual being inspected will be asked to produce courier orders (or DD Form 2501) or other documented proof of authorization to hand carry classified material. If the individual does not have such authorization, the incident will be recorded, and they will be referred to the Security Division, G3/DPTM for further action.

9. Prior to commencement of the inspection, inspector personnel will be briefed, on these procedures, by the security manager/official. Throughout the inspection period, inspector personnel are free to seek additional guidance or assistance from the activity security official.

Appendix E
Example of Courier Duties and Responsibilities Briefing

GENERAL INSTRUCTIONS:

As a designated courier of classified material, you are authorized to handcarry or escort material while traveling between your duty section and (be as specific as possible on area of limitations, i.e. Fort Knox EOC, Fort Knox DOIM, HQ TRADOC, etc.). In some situations you may not have specific knowledge of the information you are carrying. However, when you receive material in a sealed envelope or other container, you become the custodian of that information.

All government employees (military and civilian) are subject to Title 18, United States Code, which deals with unauthorized release of national security information. As a courier, you are solely and legally responsible for protection of the material in your possession. This responsibility lasts from the time you receive the material until it is properly delivered to the station, agency, activity, unit, or individual listed as the official addressee.

The intent of this briefing is to help you become familiar with your responsibilities as a courier, duties as a custodian of classified material, and the security and administrative procedures governing the safeguarding and protection of classified material. You must also familiarize yourself with the provisions of AR 380-5, paying special attention to the following areas:

ACCESS: You will be given delivery instructions for the material when it is released to you. Follow those specific instructions and seek assistance (from a responsible security official) if you are unable to do so. Dissemination of classified material is restricted to those persons who are properly cleared and have an official need of the information (need to know). No person has a right or is entitled at access classified information solely by virtue of rank or position. To help prevent unauthorized access and possible compromise of the material entrusted to you, it must be retained in your personal possession or properly guarded at all times. You will NOT read, study, display, or use classified material while in public places or conveyances.

STORAGE: Whenever classified material is not under your personal control, it will be guarded or stored in a GSA approved security container. You will NOT leave classified material unattended in locked vehicles, car trunks, commercial storage lockers, storage compartments in the passenger section of commercial transportation (plane, bus, or train). You will NOT store the material in detachable luggage racks or aircraft travel pods. You will NOT pack classified material in regular checked baggage. Retention of classified material in hotel/motel rooms or personal residences is prohibited. Safety deposit boxes and room safes provided by hotels/motels do not provide adequate protection for classified material. Advance arrangements for proper overnight storage at a US Government facility or, if in the United States, a cleared contractor facility is required prior to your departure. Arrangements are the responsibility of the activity authorizing the transmission of the classified material.

PREPARATION: Whenever you transport classified information it must be enclosed in two opaque, sealed, wrappings (envelopes, boxes, or containers) without metal bindings. While traveling, a briefcase will not be used as the outer wrapping. The inner envelope or container shall be addressed shall be addressed to an official government activity, stamped with the highest classification of the material contained, and placed inside an outer wrapping, envelope, or container. The second, or outer wrapping, envelope, or container will be sealed and addressed to the proper government agency. The second, outer wrapping, envelope, or container will NOT be stamped or marked with classification markings. Proper preparation is the responsibility of the activity authorizing transmission. Do not accept improperly prepared material for transmission. Receipts will be exchanged when an if required.

HANDCARRYING: The authorization statement contained in your orders (courier designation) should ordinarily permit you to pass through passenger control points within the United States, without the need for subjecting classified material to inspection. Except for customs inspections only, airports have established screening points to inspect all handcarried items. If you are handcarrying classified material in envelopes, you should process through the ticketing and boarding procedures in the same manner as other passengers. When the sealed envelopes are carried in briefcases, the case may be routinely opened for inspection to ensure no weapons are concealed. The sealed envelope may be checked by x-ray machine, bending, flexing, and weight. It should not be necessary for the screening official to open the envelope. If the screening official is not satisfied with your identification, authorization statement, or envelope, you will NOT be permitted to board the aircraft, and are no longer subject to further screening for boarding purposes. If you a denied boarding, contact either the activity authorizing transmission, the receiving activity, the nearest Defense Courier Service Office, the nearest US Embassy or Consulate to report your situation and request further guidance. UNDER NO CIRCUMSTANCES should you permit the screening official to open sealed envelopes or read any portion of the classified document as a condition for boarding.

ESCORTING: When escorting classified material that is sealed in a container and too bulky to handcarry or is exempt from screening, prior coordination is required with the Federal Aviation Authority and the airline involved. You will report to the airline ticket counter prior to starting your boarding process. You will be exempt from screening. If satisfied, the official will provide an escort to the screening station and exempt the container from physical inspection. If the official is not satisfied, you will not be permitted to board, and are no longer subject to further screening. UNDER NO CIRCUMSTANCES will the official be permitted to open or view the contents of the sealed container.

The actual loading and unloading of bulky material will be under supervision of a representative of the airline; however, you or other appropriate cleared persons shall accompany the material and keep it under constant surveillance during the loading and unloading process. Appropriately cleared personnel should be available to assist in surveillance at any intermediate stops, when the plane lands and when the cargo compartment is to be opened. Coordination for assistance is the responsibility of the activity authorizing the transmission of the material, but it is you responsibility to ensure this coordination has been accomplished.

Our primary concern is the protection and safeguarding of classified material from unauthorized access and possible compromise. Security regulations cannot guarantee the protection of classified material, nor can they be written to cover all conceivable situations. They must be augmented by basic security principles and a common sense approach to protection of official national security information.

You are reminded that any classified instructions you receive must also be protected. Do not discuss verbal instructions with anyone after you have delivered the material, do not talk about where you were, what you did, or what you saw.

If you have any questions concerning the security and protection of classified or sensitive material entrusted to you, contact your security manager, the activity authorizing transmission, the receiving activity, the nearest Defense Courier Service Office, or the nearest US Embassy or Consulate.

UNDERSTANDING OF COURIER DUTIES AND BRIEFING VERIFICATION
(DD Form 2501)

I,_____ have been briefed on and understand the following: (Printed Name and SSN)

1. My Courier Authorization Card (DD Form 2501) can only be used when transporting classified material by ground transportation or military aircraft.

2. The packaging requirements for classified material, as outlined in AR 380-5.

3. The custody and storage requirements for classified material, as outlined in AR 380-5.

4. I will not discuss or view classified material in public areas or with unauthorized persons.

5. I must use the most direct route to my destination.

6. My DD Form 2501 has an expiration date, and upon expiration it must be turned in to my security manager for destruction.

7. My DD Form 2501 is only valid while I am assigned to my current position, and upon release from my current position it must be turned in to my security manager for destruction.

8. I must participate in a "show" inventory of the DD Form 2501 at least semi-annually.

9. If my DD Form 2501 is lost or misplaced, I must immediately report this to my security manager.

10. I know who my security manager is and how/where to locate him/her.

11. I will immediately report any unusual incident(s) to the local Counter Intelligence Office or my security manager.

By my signature, I verify that the listed items were briefed to me and that I understand my duties and responsibilities as a courier of classified material.
I further verify that: 1) I have thoroughly read Chapter 8 of AR 380-5 and understand my responsibilities described. 2) I understand the consequences of improper or inappropriate handling of classified material while performing my duties as a courier.

SIGNATURE_____ DATE_____

UNDERSTANDING OF COURIER DUTIES AND BRIEFING VERIFICATION

(Temporary Written Authorization)

I,_____ have been briefed on and understand the following: (Printed Name and SSN)

1. My written authorization can only be used when transporting classified material by ground transportation or military aircraft.

2. The packaging requirements for classified material, as outlined in AR 380-5.

3. The custody and storage requirements for classified material, as outlined in AR 380-5.

4. I will not discuss or view classified material in public areas or with unauthorized persons.

5. I must use the most direct route to my destination.

6. My written authorization is temporary and has an expiration date, and upon expiration it must be turned in to my security manager for destruction.

7. My written authorization is only valid while I am assigned to my current position, and upon release from my current position it must be turned in to my security manager for destruction.

8. If my written authorization is lost or misplaced, I must immediately report this to my security manager.

9. I know who my security manager is and how/where to locate him/her.

10. I will immediately report any unusual incident(s) to the local Counter Intelligence Office or my security manager.

By my signature, I verify that the listed items were briefed to me and that I understand my duties and responsibilities as a courier of classified material.
I further verify that: 1) I have thoroughly read Chapter 8 of AR 380-5 and understand my responsibilities described. 2) I understand the consequences of improper or inappropriate handling of classified material while performing my duties as a courier.

SIGNATURE_____ DATE_____

Fort Knox Reg 380-5 (5 Feb 02)

Temporary Courier Authorization

Security Manager's Office Symbol (380) Date Authenticated

MEMORANDUM FOR (Office material is to be picked-up from)

SUBJECT: Authority to Hand-Carry Classified Information - Courier Designation

1. The following individual is authorized to pick-up and transport classified material including for (your organization):

   a. FULL NAME.

   b. RANK and SSN or ID Number.

   c. Type of ID.

   d. Verified Clearance Level.

   e. Pickup point. (i.e. Fort Knox EOC, USAARMC G3/DPTM, USAARMC DOIM)

   f. Limits of Authorization Area: In and around the confines of Fort Knox, Kentucky.

   g. Expiration Date. (cannot exceed 30 days from authentication date)

   h. Authority: AR 380-5, Chapter 8 and FK Reg 380-5, Chapter 8.

2. All security violations are to immediately be reported to one of the following:

   a. Security Division, G3/DPTM, 4-7076/7186/2552/7050.

   b. USAARMC SDO/SDNCO, 4-4481/4421.

3. POC is the undersigned at (security manager's phone number).

SECURITY MANAGER'S
Signature Block

CF: G3/DPTM (ATZK-PTF-D)

Appendix F
Instructions for the Completion of Standard Form 311

BLOCK #

1. Period Covered. (i.e. 1st QTR, FY 01)

2. Your Unit or Directorate

3. Security Manager or preparer's information.

4. and 5. N/A.

6. This section pertains to documents your unit or directorate created at all levels of classification. It includes Special Access Programs and Sensitive Compartmented Information. It does not to include any copies made. In order to fully understand how to fill this area out, you must understand what ORIGINAL CLASSIFICATION and DERIVATIVE CLASSIFICATION are and the difference between them.

7. This section refers to written requests that your activity review classified information for the purpose of declassifying such data. Complete the area under "Declassification Decisions," reporting the amount of pages only. Additionally, this area must be broken out into material created prior to 1976, and information created from 1976 to present. If fully or partially granted, the total should appear in Block #8.

8. Automatic declassification refers to the program established under section 3.4 of EO 12958 and amended by EO 13142, which requires that all files of permanent historical value, that will reach 25 years old by October 2001, be declassified or exempted from automatic declassification prior to 17 October 2001. We must report statistics on the amount of material reviewed, declassified, or exempted from automatic declassification, by page count. Systematic Review refers to the program under which classified, permanently valuable records, exempted from automatic declassification, are reviewed for declassification. The figures reported should indicate the combined total of pages under BOTH the systematic and automatic declassification programs. However, in Block #10, indicate the amount of material that was created after 1 January 1976. (This figure will be counted under the Systematic Declassification Program.)

9. The amount of formal inspections, surveys or program reviews you conducted on yourself or on subordinate units.

10. Include information noted above, and any other information you feel is needed to elaborate of explain any information provided.